PATENT APPLICATION
DOCKET NO. A-6307

MECHANISM AND APPARATUS FOR ENCAPSULATION OF ENTITLEMENT AUTHORIZATION IN CONDITIONAL ACCESS SYSTEM

CROSS-REFERENCE TO RELATED APPLICATIONS

Ins A

This application A1 ~~claims~~ priority to U.S. provisional application Serial No. 60/054,578, DeFreese et al., filed August 1, 1997 entitled "Mechanism and Apparatus for Encapsulation of Entitlement in Conditional Access System" ~~(Attorney Docket No. T 2910).~~

BACKGROUND OF THE INVENTION

Field of the Invention

The present invention relates to a conditional access system such as a conditional access cable television system. In particular, the invention relates to identification of packages of bundled services, called entitlement units, and the authorization of reception of an entire entitlement unit.

Description Of Related Art

Known conditional access systems individually authorize each service to be received. For example, a subscriber of a cable television system may subscribe to a plurality of services (e.g., HBO, Cinemax, ShowTime, etc.).

Known conditional access systems provide services to subscribers in tiers. Tiers are used as a way to provide standard service to some subscribers while providing premium services to other subscribers. Each subscriber is assigned to a specific tier. For example, consider a service that provides two tiers: a standard service that carries over the air broadcast programs and a premium service that carries the standard service plus HBO, Cinemax and ShowTime. Tier authorization data is transmitted from the system's headend to a home communication terminal for each subscriber where it is stored. In this example, the tier authorization data may be a single bit set to indicate premium service and cleared to indicate standard service. In general, many tiers (e.g.,.256) may be provided. The tier authorization data may be a number (e.g., from 0 to 255) that indicates the authorized tier. Each tier corresponds to a specific combination of authorized programs out of a list of available programs (e.g., out of 128 available programs). Alternatively, the tier authorization data may be a long data word (e.g., 128 bits or 16 bytes of 8 bit each) where each bit in the tier authorization data corresponds to an authorized program. The tier authorization data in this example is merely the long data word with as many bits set as there are authorized programs for the tier, and the identification of the authorized programs is by noticing the bit position that is set.

No matter how the tier authorization data is encoded, it is transmitted from the headend to a subscriber's home communication terminal. Each subscriber is authorized for a particular tier. A table that relates the tier authorization data for each subscriber to the correspondingly identified home communication terminal is stored in the headend. For each subscriber, the headend prepares a unique addressed message containing the tier authorization data corresponding to the subscriber, and the headend transmits the data to the subscriber's home communication terminal. Often the data is encrypted by the headend and decrypted by the home communication terminal.

Programs broadcast from the headend are identified by frequency, channel number, digital data stream number, etc. The home communications terminal processes a subscriber's request for a particular program by determining a number associated with the requested program and verifying that the terminal is authorized to receive a tier that "contains" the program.

BRIEF DESCRIPTION OF DRAWINGS

The invention will be described in detail in the following description of preferred embodiments with reference to the following figures wherein:

FIG. 1 is a block diagram of the communication system according to the invention;

FIG. 2 is a block diagram of a terminal according to the invention;

FIG. 3 is a block diagram of a processor of the terminal according to the invention;

FIG. 4 is a format diagram of a packetized data transport stream (a multiplex) as processed by the invention;

FIG. 5 is a flow chart of a method of determining whether a service is authorized according to the invention;

FIG. 6 is a flow chart of a method of pre-confirming authorization; and

FIG. 7 is a flow chart of a method of post-confirming authorization.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

In FIG. 1, a conditional access communication system includes headend 2, a plurality of home communication terminals 4, and a link therebetween 6. The headend operator may receive content for transmission from a plurality of service providers 8.

In FIG. 2, terminal 10 (e.g., as included in home communications terminal 4) includes processor 20, tunable tuner 12, demodulator 14, and control link 16 to control the frequency of tunable tuner 12. Terminal 10 may also include second tuner 22 and demodulator 24 to receive "out of band" data streams.

In operation, headend operators provide a plurality of services. Usually each service is carried on a separate 6 MHZ channels. To receive a particular service, processor 20 directs tunable tuner 12 by control link 16 to tune to the frequency of the particular service desired. Demodulator 14 demodulates the tuned signal according to its modulation technique (e.g., PSK, QPSK (Quadrature Phase Shift Keying Modulation), Offset QPSK, etc.). Standards have been developed for carrying wideband video and audio information for a program (e.g., MPEG-2). However, some systems may carry non-MPEG (Moving Picture Experts Group) compliant signals (e.g., IP packets). When this occurs, terminal 10 may include second tuner 22 and demodulator 24 to recover non-MPEG compliant data. Both data streams are processed in processor 20, or separate but coupled processors may be provided.

In FIG. 3, a more detailed description of processor 20 is depicted. Processor 20 includes secure microprocessor 30 and individual service decryptors 60. Processor 20 also includes demultiplexer 22 to cull encrypted and/or authenticated entitlement control message 28 from the transport data stream input and to cull encrypted entitlement management message 52 from the transport data stream input. Demultiplexer 22 also culls clear payload text 68 from the transport data stream which is provided to service demultiplexor 26. The transport data stream (TDS) is also provided at 24 to service demultiplexor 26 and may include video signals, a plurality of audio signals, or utility information. Any or all of these separate information data streams may be separately encrypted. If these information data streams are separately encrypted they will be decrypted, if authorized, in service decryptor 60 as discussed below.

Secure microprocessor 30 includes secure memory 38 that stores multi-session key (MSK), entitlement unit number and a decoder private key (DPK). Secure microprocessor 30 also includes decryptor 32, decryptor and/or authenticator 34, conditional access logic 36 and authorized control word decryptors 40. Decryptors 32 and 40, decryptor and/or authenticator 34 and conditional access logic 36 may advantageously be implemented in a general purpose arithmetic/logic section and program memory section (having a program stored therein) of secure microprocessor 30. Secure microprocessor 30 is characterized by memory 38 being unobservable at the input/output terminals of secure microprocessor 30. Thus, any intermediate unencrypted data may be stored in memory 38 (preferably non-volatile) without being observable by pirates. Data transferred into or out of secure microprocessor 30 is preferably protected at the terminals of microprocessor 30 by encryption if the data is long lived or remains unprotected if the data is so short lived that its observation by a pirate is harmless. For example, multi-session key is preferably stable for a period of hours to a month or so. Thus, it is preferably encrypted. In contrast, control words that are decrypted in secure microprocessor 30 from encrypted entitlement control messages typically change every 2 to 5 seconds so that observation of the control word by a pirate does not seriously compromise the system's security.

When entitlement control messages are transported in the transport data stream in encrypted form, a pirate is unable to observe the entitlement unit numbers and control words contained in the entitlement control message. However, the entitlement control message may also be transported in authenticated form (e.g., keyed secure hash). In authenticated form, the entitlement control message includes two parts: a clear text part and a hashed part. The entitlement control message is authenticated in authenticator 34 of secure microprocessor 30 (FIG. 3) by hashing the clear text part and comparing it to the hashed part of the entitlement control message. If they agree, then the entitlement control message is authenticated. A pirate may be able to observe the clear text part of the entitlement control message; however, if a pirate were to attempt to insert an additional entitlement unit number into the entitlement control message, the comparison of the hashed part and the results of the local hashing will fail. This reveals a modification of the entitlement control message, and the modified message is ignored.

In operation, demultiplexor 22 culls encrypted entitlement management message 52 from the transport or "out of band" data stream and provides it to decryptor 32. Decoder private key is read from secure memory 38 passed through conditional access logic 36 to decryptor 32 where it is used to decrypt and/or authenticate entitlement management message 52. Decoder private key may be a secret key such as those used in the Data Encryption Standard (DES) algorithm or must be the private component of a public/private key pair such as those used in the RSA algorithm. The entitlement management message includes both authorized entitlement unit number to be stored in secure memory 38 and authorized multi-session key to be stored in secure memory 38. Multi-session key is changed from time to time, preferably monthly or more often. When a subscriber wishes to upgrade service and be authorized to receive additional services (e.g., change from HBO only to HBO and Cinemax), a new entitlement management message will be transmitted to the secure microprocessor so that a new entitlement unit number will be recovered by decryptor 32 and stored in secure memory 38.

Encrypted and/or authenticated entitlement control message 28 is culled from the transport data stream input and provided to decryptor and/or authenticator 34. Multi-session key is read from secure memory 38 and passed through conditional access logic 36 to decryptor and/or authenticator 34 at 46. Decryptor and/or authenticator 34 decrypts and/or authenticates the entitlement control message to reveal encrypted control words for each encypted component (e.g., video, audio, etc.) of the service being carried on the transport data stream and to reveal a list of all entitlement unit numbers to which the currently received service belongs. For example, a first entitlement unit may include both HBO and Cinemax, whereas a second entitlement unit may include only HBO. The entitlement control message for the HBO service (i.e., HBO data stream) would include both the first and second entitlement unit numbers.

Conditional access logic 36 compares the list of entitlement unit numbers from decryptor and/or authenticator 34 with the authorized entitlement unit number stored in secure memory 38. If there is a match, then the service may be received. Conditional access logic 36 will then pass the control words from the decrypted and/or authenticated entitlement control message to the decryptors 40. Control words for individually encrypted service components (e.g., video, audio, etc.) are passed to decryptor 40. In decryptor 40, the control words will be decrypted using the multi-session key to provide clear text versions of the control words, or “service seeds” 62.

Control words are characterized by frequent changes. Whereas, multi-session key may change as infrequently as once a month, control words may change every two to five seconds. The decrypted control words are provided by decryptor 40 at output terminals of secure microprocessor 30. Even if a pirate were to recover a decrypted control word, the decrypted control word is short lived so as to have substantially no value to the pirate.

Service selection data 56 from the decrypted contents from decryptor and/or authenticator 34 is provided to service demuliplexor 26 via control access logic 36. Selected services 64 are provided by service demultiplexor 26 to service decryptor 60 at 64 based on service selection 56. Service decryptor 60 processes encrypted services of the selected services 64 using seeds 62 to provide decrypted services 66.

In FIG. 4, a representative transport data stream 70 (called a multiplex) is depicted. The transport data stream is packetized in packets of 188 bytes. Each packet includes a synchronization block and a prefix. Payload data may be concatenated between a plurality of transport packets to form a packetized elementary stream as depicted at the top of FIG. 4. One packetized elementary stream depicted at the bottom of FIG. 4 is the network information table (NIT). The network information table carries such information as a table of direct correspondence between a multiplex number and a frequency (for tuner 12 of FIG. 2) in which the data stream may be found.

Other information may be provided with the network information table. For example, entitlement unit table (EUT) in which each service, identified by universal service identification number (USID) is included together with each entitlement unit number to which the service belongs. Alternatively, the entitlement unit table may be transported “out of band” and received in processor 20 via tuner 22 and demodulator 24 (FIG. 2).

Similarly, in order to aid a user to select a desired service, service information may be provided over a permanently available data link (e.g., a data link not switched with the selected program) as either “in band” or “out of band” data. For example, an out of band data link may be a 108 MHz phase shift keyed (e.g., QPSK) broadcast data link. In band might be specific data packets in the data stream at a predetermined initial tuned frequency. Permanently available in band data link data might also be data packets carried in the data stream of all tunable frequencies. Such service information provides a list of services (i.e., universal service identification numbers) corresponding to each data stream number. Preferably, additional text is carried with the service information for each service so as to enable the terminal to include a electronic program guide.

In FIG. 4, program association table (PAT) is carried as payload data in packet 0 of multiplex 70. The program association table includes a list of each program available and a corresponding packet number at which program map table (PMT) may be found. There is a program map table for each program. The program map table includes a list of each component of the program (e.g., audio and video, entitlement control messages, etc.) and a packet number at which the program component (e.g., audio, video, entitlement control messages, etc.) may be found. Of particular importance is the program component that is the entitlement control message since it specifies all entitlement unit numbers to which the program belongs. The program map table includes information directing where the entitlement control message for that program may be found. This enables demultiplexor 22 (FIG. 3) to cull the encrypted entitlement control message 28 from the transport data stream.

Also of importance is conditional access table (CAT) found in packet 1 of multiplex 70 (FIG. 4). The conditional access table has for each system type of secure microprocessor (e.g., 30 in FIG. 3) in the system, a packet identification number where the encrypted entitlement management messages may be found. This packet number enables demultiplexor 22 to cull the encrypted entitlement management message 52 from the transport data stream (FIG. 3). Further filtering based on the address of the secure micro-processor may then be performed.

In FIG. 5, method 100 for determining whether a terminal is authorized to receive a service is practiced in processor 20 (FIG. 2). At step 102 data is read from the data stream. This data includes the entitlement unit table and the service information. At step 104, a user selects a desired service associated with a universal service identification number (e.g., as may be used with an electronic program guide). This may be accomplished through any of the known electronic program guide techniques. The entitlement unit table from the network information helps translate the universal service identification number into entitlement unit numbers that belong to the service. At step 110, the secure microprocessor pre-confirms whether the authorized entitlement unit number stored in secure memory 38 (FIG. 3) is a member of the entitlement unit numbers in the entitlement unit table that corresponds to the selected service. If it is not a member, at step 106, a message may be displayed to the user (e.g., displayed on a television style monitor) and the user will be requested to select another service. Alternatively, the terminal may automatically step to the next service, or to any predetermined service such as a barker channel.

It will be noted that a service pirate may attempt to add extra entitlement unit numbers to the entitlement unit table. However, based on the present invention, the pirate will still be unable to recover the service.

When it is determined at step 110 that a service is authorized, at step 124, tuner 12 is directed to tune to the desired service. This information comes from the network information table that associates the universal service identification number with the frequency on which the service may be received. After tuner 12 tunes to the correct frequency, demodulator 14 recovers the digital data stream carried at the tuned frequency. At step 130 (FIG. 5), the digital data stream is decrypted. At step 150, the decrypted digital data stream is decompressed (e.g., decompression from the compressed MPEG format) and then displayed to the user.

Step 110 (FIG. 5) is further described with reference to FIG. 6. The entitlement unit table has a list of all entitlement unit numbers that carry the specified service. In a loop that includes steps 112, 114, 116, 118 and 120, all entitlement unit numbers from the entitlement unit table are tested. At step 112, the first (and in later iterations the next) entitlement unit number belonging to the selected service is read from the entitlement unit table. At step 114, the entitlement unit number from the entitlement unit table is sent to the secure microprocessor to be compared to the authorized entitlement unit number stored in secure memory 38 (FIG. 3). If the comparison is favorable, then the service is declared authorized at step 116, and the tuner tunes to the service (step 124, FIG. 5). If the comparison is unfavorable, then at step 118, a test is made to determined whether all entitlement unit numbers from the entitlement unit table have been tested. If all entitlement unit numbers from the entitlement unit table have been tested and none has been the authorized entitlement unit number stored in secure memory 38, then the service is declared not authorized. However, if there are still more entitlement unit numbers from the entitlement unit table to be tested, then the next entitlement unit number is read in steps 120 and 112, and the loop is repeated.

This pre-tuning testing procedure has human factors benefits. Subscribers who tend to "surf" through the channels will tend to grow impatient if the time required to produce a› display exceeds 1 second, and this delay will be relatively unnoted if the time to produce the display is less than 1/4 of a second. If is therefore desirable to provide a quick way to determine whether a service is authorized or unauthorized before tuner 12 is directed to tune to a particular frequency. It should be noted that the entitlement unit table may not be, and is not required for this purpose, to be secure. It may be sent unencrypted.

In FIG. 7, decrypting the service in step 130 is described in more detail. Processor 20 preferably includes a general purpose microprocessor performing step 132. Step 132 includes acquiring program association table and program map table at step 134.

At step 136, the general purpose microprocessor directs demultiplexor 22 to cull the encrypted and/or authenticated entitlement control message 28 (FIG. 3) from multiplex 70 (FIG. 4). The encrypted and/or entitlement control message is then sent to secure microprocessor 30 (FIG. 3) to be decrypted and/or authenticated.

At step 140, the encrypted and/or authenticated entitlement control message is decrypted and/or authenticated in the secure microprocessor, and the authorized entitlement unit number stored in secure memory 38 (FIG. 3) is compared to the list of entitlement unit numbers to which the present desired service belongs as listed in the decrypted and/or authenticated entitlement control message. This confirmation process takes place after tuner 12 tunes to the desired frequency. Since the entitlement control message is encrypted and/or authenticated, a pirate would not be able to insert false entitlement unit numbers into the entitlement control message without be detected.

When it is confirmed that the authorized entitlement unit number (stored in secure memory 38) is the same as one of the entitlement unit numbers carried in the entitlement control message, one or more control words are recovered from the entitlement control message. These control words correspond to each individual component of the service and are provided at 50 to decryptor 40 (FIG. 3). The control words are decrypted using multi-session key in decryptor 40 to provide seeds for decryption of service components in service decryptor 60.

In step 138 (FIG. 7), service selection data 56 (FIG. 3) from the decrypted and/or authenticated entitlement control message is used by service demultiplexor 26 (FIG. 3) to pass encrypted service component data 64 (e.g., audio or video) to service decryptor 60. In step 142 (FIG. 7), service decryptor 60 decrypts the encrypted service component data 64 using decrypted control words as seeds 62 from decryptor 40 to provide decrypted service components 66 (FIG. 3).

Thus, before tuner 12 (FIG. 2) is tuned, an initial fast, albeit possibly unsecured, determination is made as to whether the selected service is authorized as one of the services covered by the authorized entitlement unit number stored in secure memory 38. If the selected service appears to be an authorized service, then tuner 12 is tuned to the specified frequency and the transport data stream from that specified frequency is processed. In the transport data stream corresponding to the specified frequency is an encrypted and/or authenticated entitlement control message. It is this entitlement control message that is decrypted and/or verified in secure microprocessor 30 in order to reveal, in a secure environment, the entitlement unit numbers that belong to the service. The secure microprocessor compares the list of entitlement unit numbers from the entitlement control message against the authorized entitlement unit number in memory 38 in order to determine whether the service reception is authorized in a secure microprocessor unobservable to pirates.

Since decryption is not required prior to tuning, the pre-tuning steps are performed with great dispatch. A pirate may be able to insert false entitlement unit numbers into the entitlement unit table, but not into the encrypted entitlement control message. Even though a pirate may insert a false entitlement control message into the data stream, it will not be an authenticated entitlement control message, The authentication process carried out in authenticator 34 (FIG. 3) will reveal the deception and the false entitlement control message will be disregared. Thus, all that a pirate can accomplish is a slowing of the speed at which a user may surf through the channels.

In another embodiment, entitlement control messages are located by index. Entitlement control messages are sent in the MPEG transport stream to provide conditional access information for a given MPEG program. In this embodiment, all entitlement control messages for a given MPEG program are packed into one MPEG PID stream. This reduces the bandwidth required to transmit the entitlement control messages. Separate entitlement control messages are still associated with respective elementary streams (e.g., video or audio) by use of the stream_index discussed below.

Entitlement control messages bearing MPEG packets are mapped to the program elements (e.g., video and each audio data stream) of an MPEG program using a conditional access descriptor (CA_descriptor) as elementary stream (ES) information in the program level of the transport stream program map section. The CA_descriptor identifies the entitlement control message PID that carries all of the conditional access entitlement control messages pertaining to the elementary stream associated with the extended ES information. The CA_descriptor carried in the program map table used as extended ES information includes: a descriptor_tag, a descriptor_length, a CA_system_ID, a CA_PID, and an ECM_information_descriptor. The descriptor_tag is preferably an 8 bit field defined by MPEG standards to be 0x09 indicating that the CA_descriptor is for a conditional access system. The descriptor_length is preferably an 8 bit field representing the number of bytes (or bits, etc.) of the present CA_descriptor. The CA_system_ID is preferably a 16 bit field identifying the particular conditional access system to which the CA_descriptor pertains. There may be more than one. The CA_PID is preferably a 13 bit field carrying the PID value of the entitlement control message bearing packets for the associated elementary stream. The ECM_information_descriptor preferably includes one or more 24 bit fields (the number depends on descriptor_length, above) where each 24 bit field includes: an ECM_descriptor_tag, an ECM_descriptor_length, and a stream_index. The ECM_descriptor_tag is an 8 bit field that identifies a characteristic of the associated entitlement control message, for example, identifying the entitlement control message as a stream type descriptor (other descriptor types being possible). The ECM_descriptor_length is an 8 bit field that merely identifies the remaining length of the current ECM_information_descriptor (in bytes). The stream_index is an 8 bit field that identifies the entitlement control messages in a multiple entitlement control message stream that contain information pertaining to the elementary stream associated with the CA_descriptor.

Entitlement control messages for all elementary streams (e.g., video, audio, etc.) of a given program are packed into packets identified by one PID. For example, assume that an MPEG program has (1) a video stream identified by PID 100, an audio stream identified by PID 200, and an entitlement control message stream identified by PID 300. PID 300 contains entitlement control messages used by both the video and audio data streams. The entitlement control messages for each elementary stream are assigned arbitrary but unique and preferred sequential stream index values. For example, entitlement control messages for the video stream (PID 100) may be assigned a stream_index value of 25, and entitlement control messages for the audio stream (PID 200) may be assigned a stream_index value of 50.

The information contained in the transport stream program map table is used to link entitlement control messages to the correct elementary stream. The CA_descriptor (described above) is looked up in the program map table when the program is selected. For the present example, the program map table identifies the video stream as PID 100 and the audio stream as PID 200. The program map table identified the CA_descriptor which in turn identifies the CA_system_ID, the CA_PID as 300 (in this example) and the stream_index for the video as 25 and for audio as 50 as discussed above. Thus, home communication terminal 4 (FIG. 1) can identify the PID of the video and audio streams from program map table. Further, home communications terminal identifies one PID (using the CA_descriptor discussed above) for all entitlement control messages associated with the present program. However, it is still possible to maintain separate entitlement control messages for each elementary stream by using the stream_index (as discussed above) for each separate elementary stream.

Having described preferred embodiments of a novel apparatus and method for the encapsulation of entitlement authorization in a conditional access system (which are intended to be illustrative and not limiting), it is noted that modifications and variations can be made by persons skilled in the art in light of the above teachings. It is therefore to be understood that changes may be made in the particular embodiments of the invention disclosed which are within the scope and spirit of the invention as defined by the appended claims.

Having thus described the invention with the details and particularity required by the patent laws, what is claimed and desired protected by Letters Patent is set forth in the appended claims.